INFOARMOR
DETECTION IS THE NEW PREVENTION

GovRAT

Advanced Persistent Threats

DIGITAL CERTIFICATES FOR SALE IN THE UNDERGROUND

NOVEMBER 2015

INFOARMOR
DETECTION IS THE NEW PREVENTION

Content

NOVEMBER 2015

INFOARMOR
HAS IDENTIFIED A NEW TREND:

Underground vendors selling digital certificates for malware code signing.

Introduction

INFOARMOR
DETECTION IS THE NEW PREVENTION

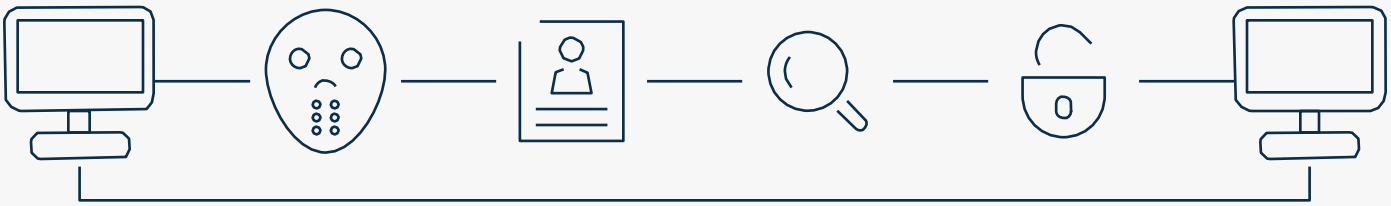
What is a Digital Certificate and Code Signing?

A digital certificate is an electronic passport allowing people, computers or organizations to exchange secure information over the Internet using the public key infrastructure (PKI). PKI is a highly secure method for exchanging information based on public key cryptography. The foundation of a PKI is the Certificate Authority (CA), which issues digital certificates that authenticate the identity of organizations and individuals over the Internet. These digital certificates are also used to sign messages (known as code signing), which ensures that messages have not been tampered with.

Windows, Mac OS X, and most Linux operating systems provide updates using code signing to ensure malicious code cannot be distributed via a patch system. Code signing also allows the receiving operating system to verify that the update is legitimate, even if the update was delivered by a third party or physical media.

Advanced Persistent Threat (APT): The Role of Digital Certificates

An advanced persistent threat (APT) is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time.



The intention of an APT attack is to steal data rather than damage the network or organization.

Bad actors use advanced technologies and encryption to create undetectable APT's.

Digital certificates and code signing may help to make malware more undetectable by modern security solutions.

Signed binary code is interpreted as potentially trusted and verified software, which allows it to slide under the radar of antiviruses and proactive defense systems.

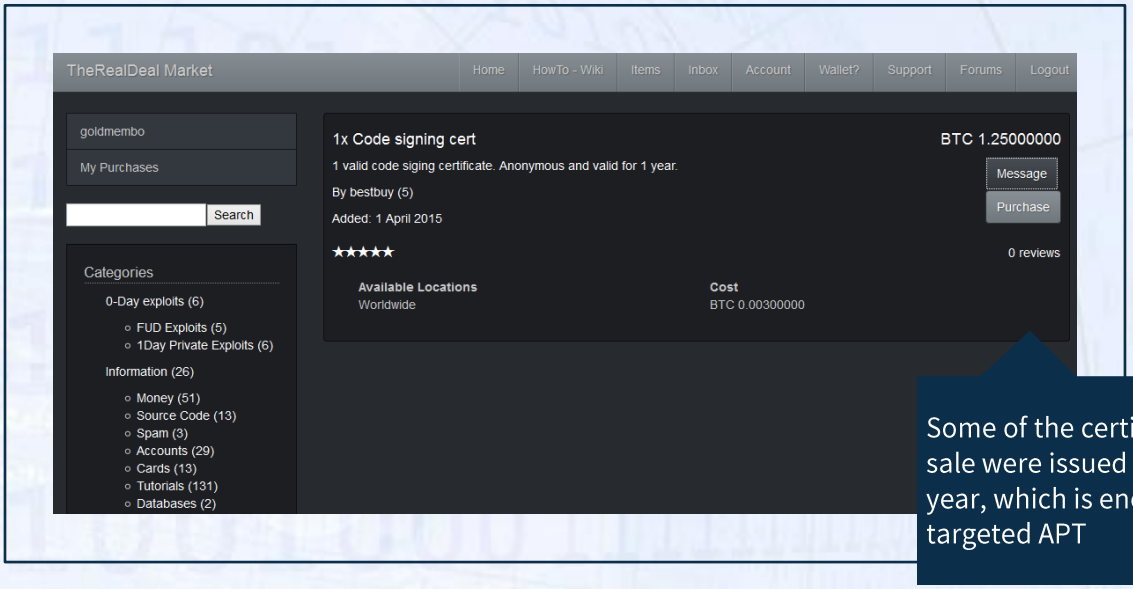
Such techniques using stolen or fake digital certificates were discovered in the Stuxnet worm, the Sony hack, and many state-sponsored targeted cyber attacks against major brands, government agencies and military organizations around the world.

GovRAT Malware Analysis

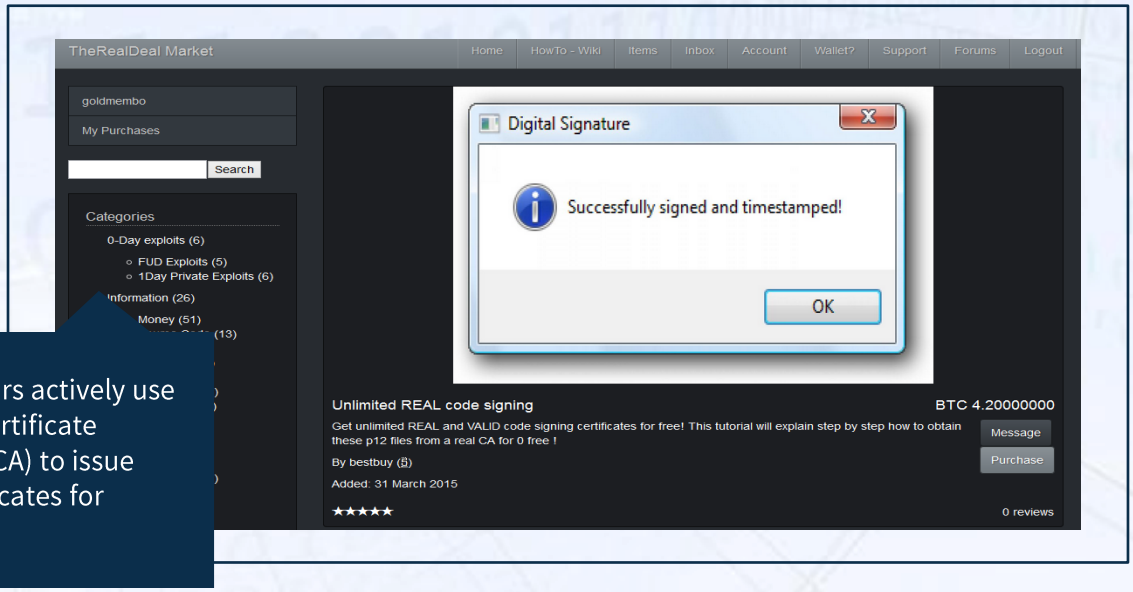
INFOARMOR
DETECTION IS THE NEW PREVENTION

GovRAT – "Excellent for long term campaigns"

InfoArmor has identified a new trend: underground malware vendors selling digital certificates for code signing, which adds a new dimension to the threat.



Some of the certificates for sale were issued just for 1 year, which is enough for targeted APT



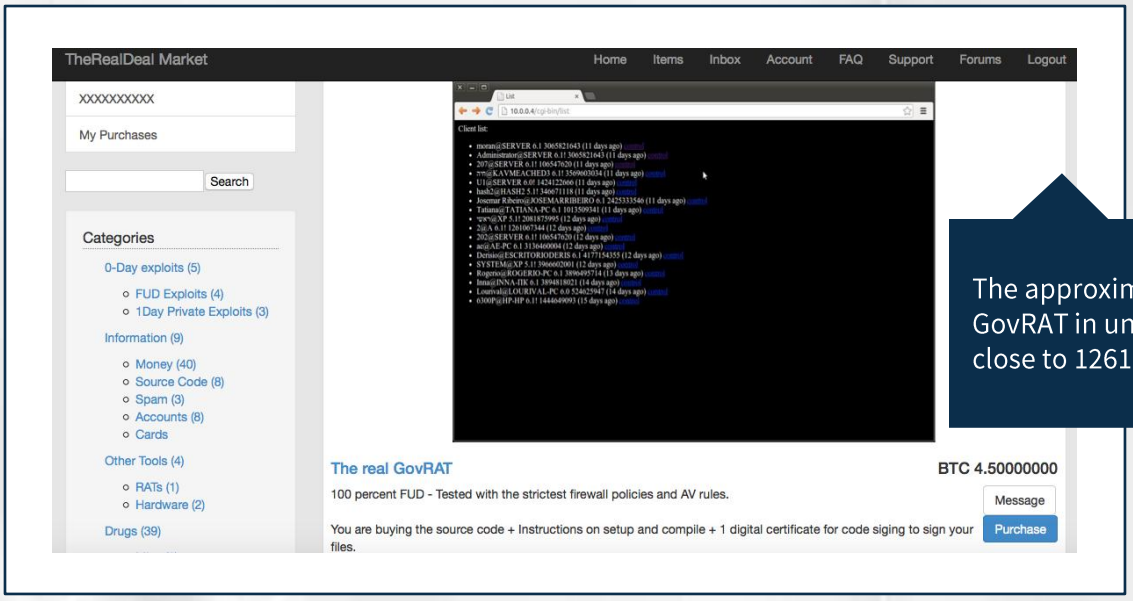
The bad actors actively use legitimate certificate authorities (CA) to issue digital certificates for malware

GovRAT is malware that is bundled with digital certificates for code signing and then sold on TheRealDeal Market, a famous underground marketplace in the TOR network. Tor directs Internet traffic through a free, worldwide, volunteer network to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.

GovRAT's Features

INFOARMOR
DETECTION IS THE NEW PREVENTION

The likely intention of **GovRAT** malware is to use it in advanced cyber espionage APT campaigns. This is touted in a description by the author under the nickname “bestbuy,” claiming “Excellent for long term campaigns”.



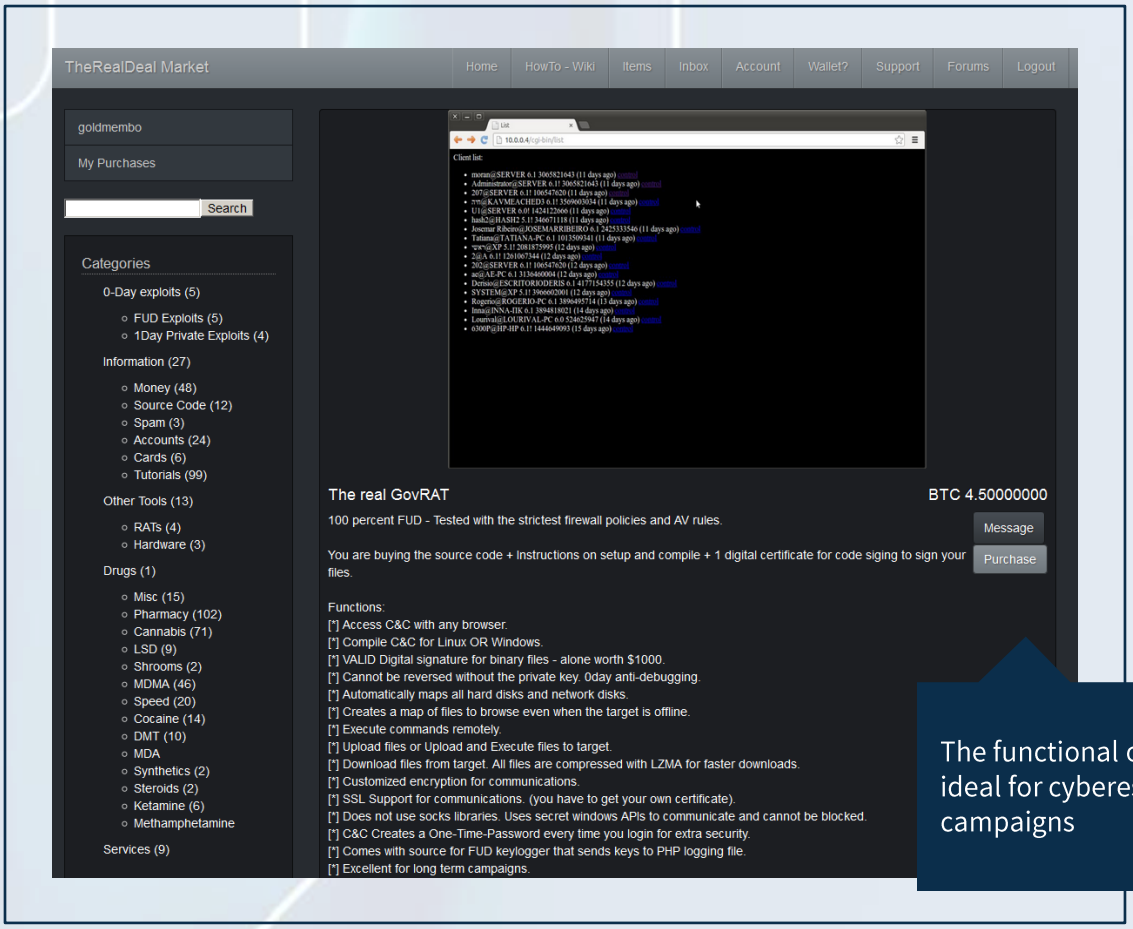
The description of **GovRAT** indicates that the malware is loaded with advanced features for potential cyber espionage:

- Access C&C with any browser.
- Compile C&C for Linux or Windows.
- VALID Digital signature for binary files - alone worth $1,000.
- Cannot be reversed without the private key. 0 day anti-debugging.
- Automatically maps all hard disks and network disks.
- Creates a map of files to browse even when the target is offline.
- Execute commands remotely.
- Upload files or Upload and Execute files to target.
- Download files from target. All files are compressed with LZMA for faster downloads.
- Customized encryption for communications.
- SSL Support for communications (you have to get your own certificate).
- [*] Does not use socks libraries. Uses secret windows APIs to communicate and cannot be blocked.
- [*] C&C Creates a One-Time-Password every time you login for extra security.
- [*] Comes with source for FUD keylogger that sends keys to PHP logging file.
- [*] Excellent for long-term campaigns.

GovRAT's Features

INFOARMOR
DETECTION IS THE NEW PREVENTION

Once the malicious agent with digital signature is planted on the victim's device, it bypasses modern antivirus software, uses the SSL connection for encrypted communications, and complicates the traffic from the victim to C&C to obfuscate analysis.



The functional of GovRAT is ideal for cyberespionage campaigns

Reverse engineering of the malware sample showed that **GovRAT** uses sandbox detection by disk volume serial numbers.

In many sandboxes the volume serial number is static since they are virtualized copies of the original system image.

Right after the identification of “magic number”, used by one of the known malware analysis platforms, the malware will finish its work without any payload execution in order not to be detected.

Victim Analysis

INFOARMOR
DETECTION IS THE NEW PREVENTION

1 Certificate Per APT

In most cases, the bad actors have used one certificate per malware sample, signing each binary individually.

15+ Governments

The identified GovRAT victims showed the target to infect various political, diplomatical and military employees of more than 15 governments around the world.

7 Financial Institutions

Several attacks were identified against leading financial institutions, including top US based banks.

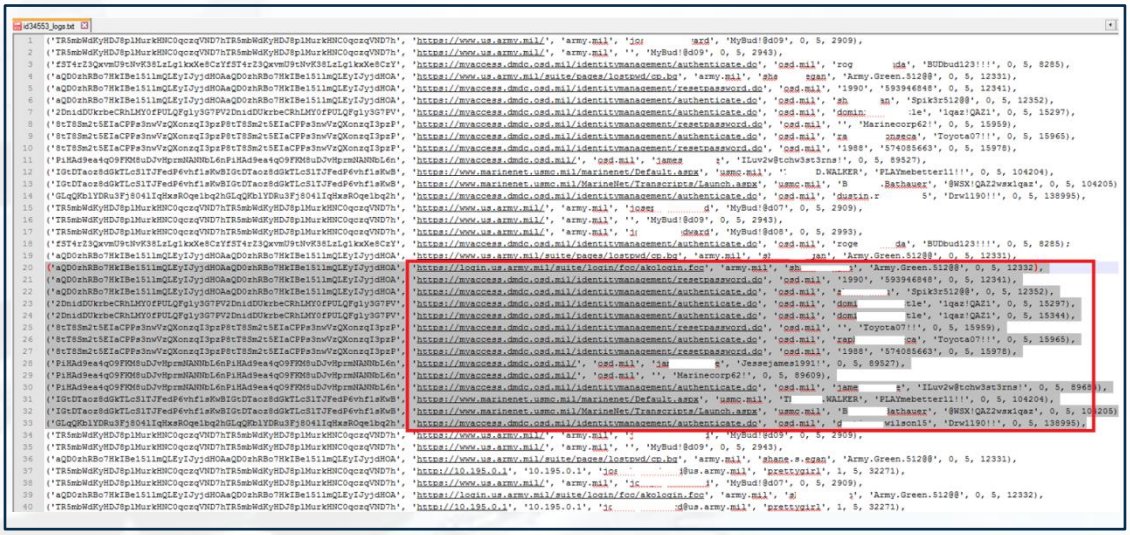
30+ Defense Subcontractors

One of the key targets of the GovRAT campaign were defense subcontractors, their current trade plans, solutions, and contracts.

100+ Corporations

In addition to government targets, large corporations in a wide variety of industrial sectors have been under attack by GovRAT since early in 2014.

Victim Analysis



After successful data exfiltration from one of the identified GovRAT botnets, several compromised accounts and infected network hosts belonging to the employees of US Army, Defense Manpower Data Center (DMDC) and United States Marine Corps (USMC) were identified.

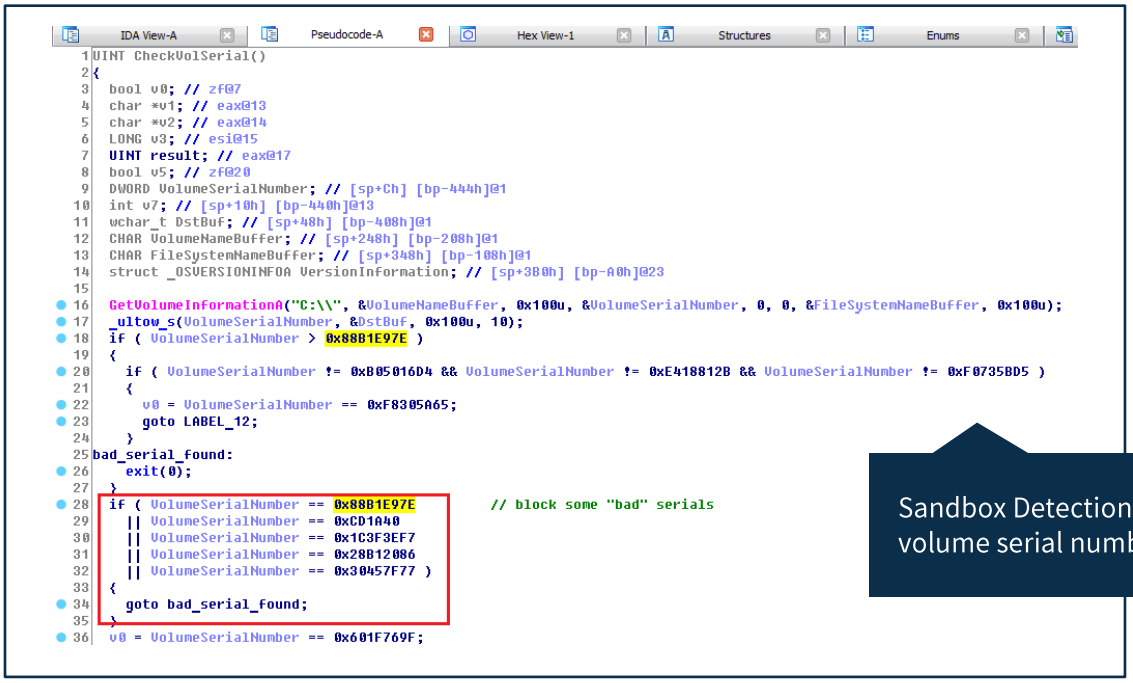
The InfoArmor Threat Intelligence team believes the interests of the bad actors are potentially concentrated on personal data and credentials of the military community members who have access to classified or internal documents and systems such as MarineNet.

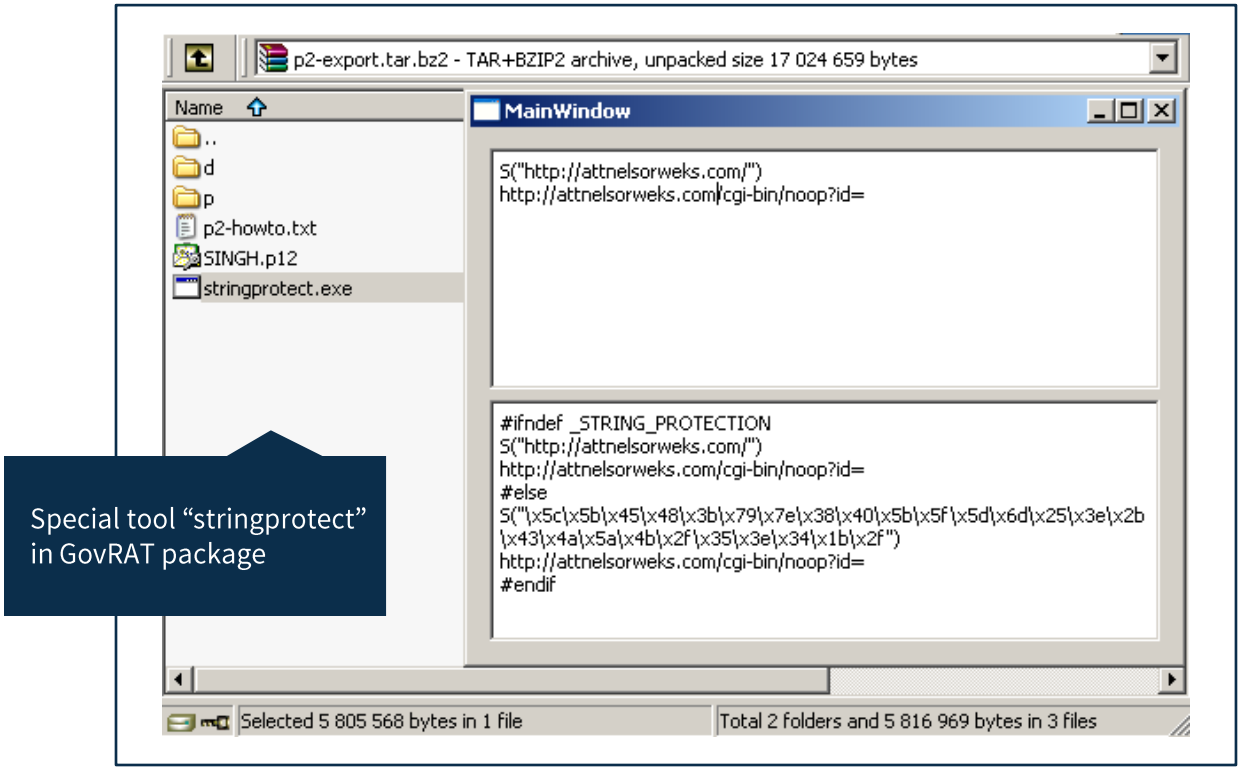
This data is very valuable for intelligence agencies analyzing trends and methodologies of foreign military forces for use in strategic analytics and cyberespionage.

Advanced Sandbox Detection

INFOARMOR
DETECTION IS THE NEW PREVENTION

GovRAT leveraged advanced anti-debugging techniques based on strings decryption, which makes the malware analysis process very complicated. Besides the use of a digital certificate for code signing, it also uses a special executable tool “stringprotect.exe”, used for strings obfuscation in order to prevent static analysis, using the encryption key as a part of the malicious file name.





Advanced Sandbox Detection

INFOARMOR
DETECTION IS THE NEW PREVENTION

GovRAT AUTHOR:

Extra info:
==========

This is a very big and complex code. Not the every-day script kiddie quality. If you are making changes to it there are some things you should be aware of:

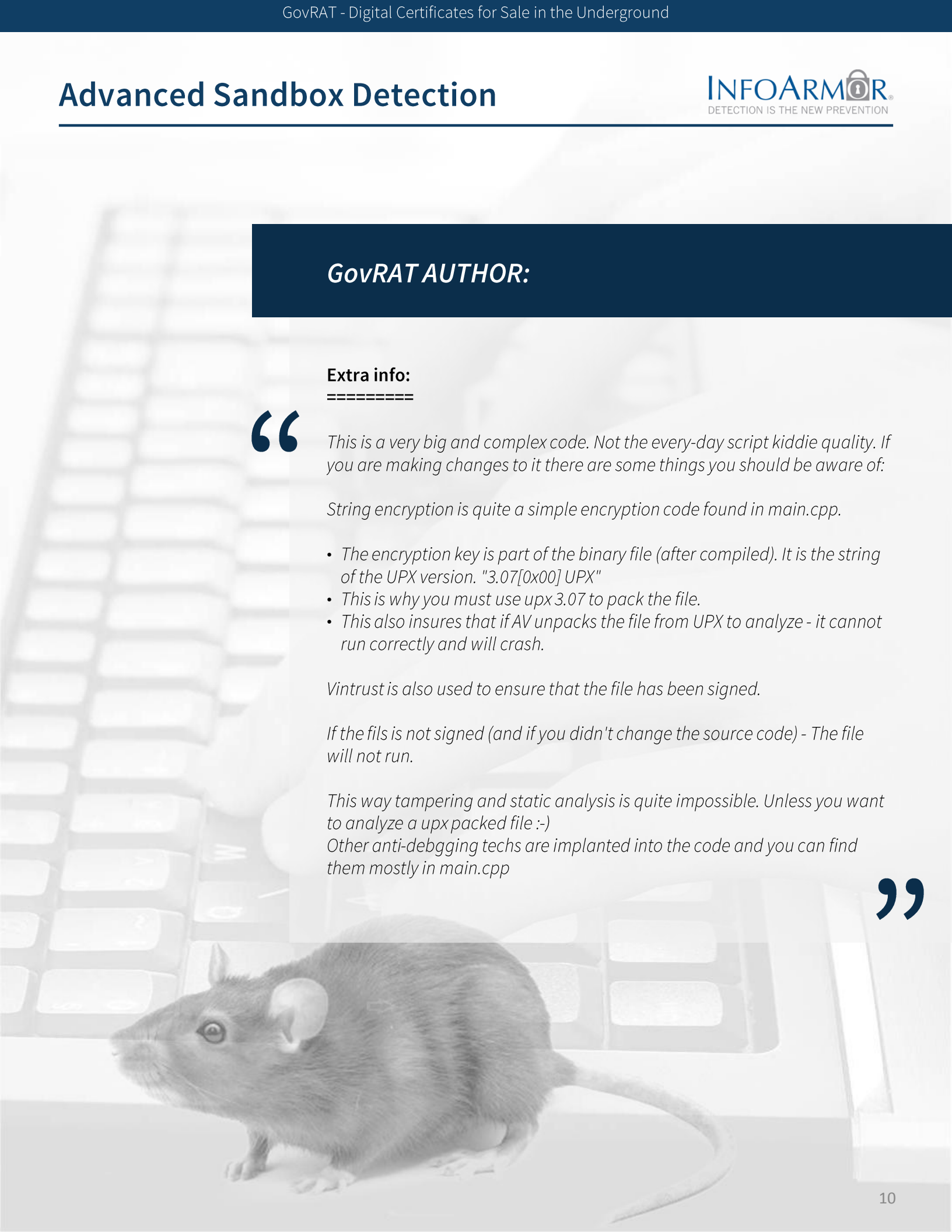
String encryption is quite a simple encryption code found in main.cpp.

- *The encryption key is part of the binary file (after compiled). It is the string of the UPX version. "3.07[0x00] UPX"*
- *This is why you must use upx 3.07 to pack the file.*
- *This also insures that if AV unpacks the file from UPX to analyze - it cannot run correctly and will crash.*

Vintrust is also used to ensure that the file has been signed.

If the fils is not signed (and if you didn't change the source code) - The file will not run.

This way tampering and static analysis is quite impossible. Unless you want to analyze a upx packed file :-)
Other anti-debgging techs are implanted into the code and you can find them mostly in main.cpp



Self-Encryption& Anti-Debugging

INFOARMOR
DETECTION IS THE NEW PREVENTION

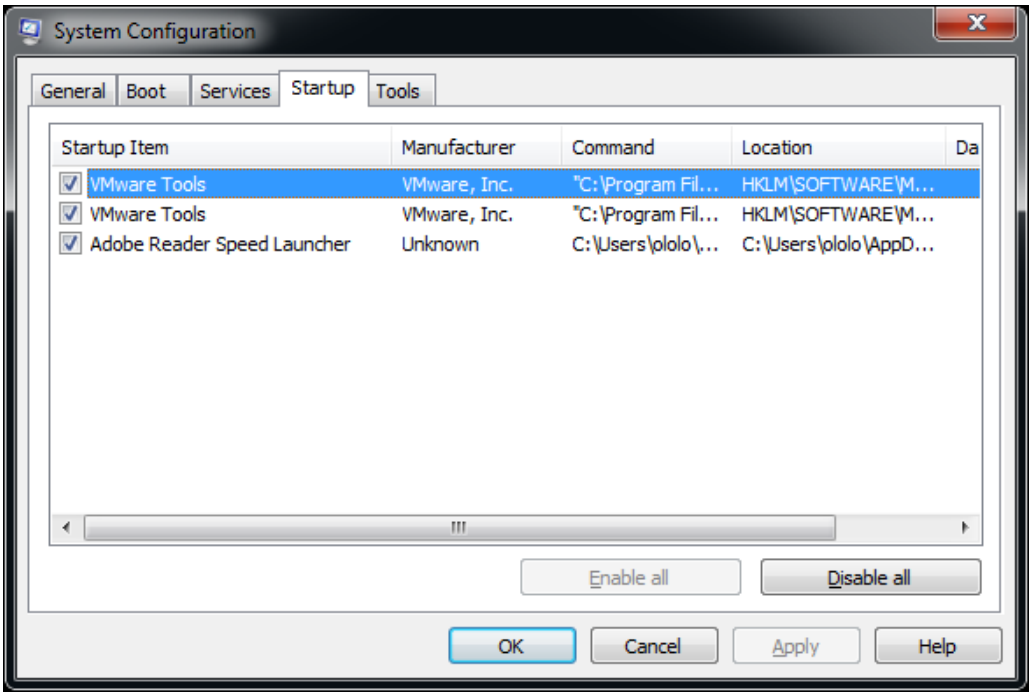
IDA View-A | Pseudocode-A | Hex View-1

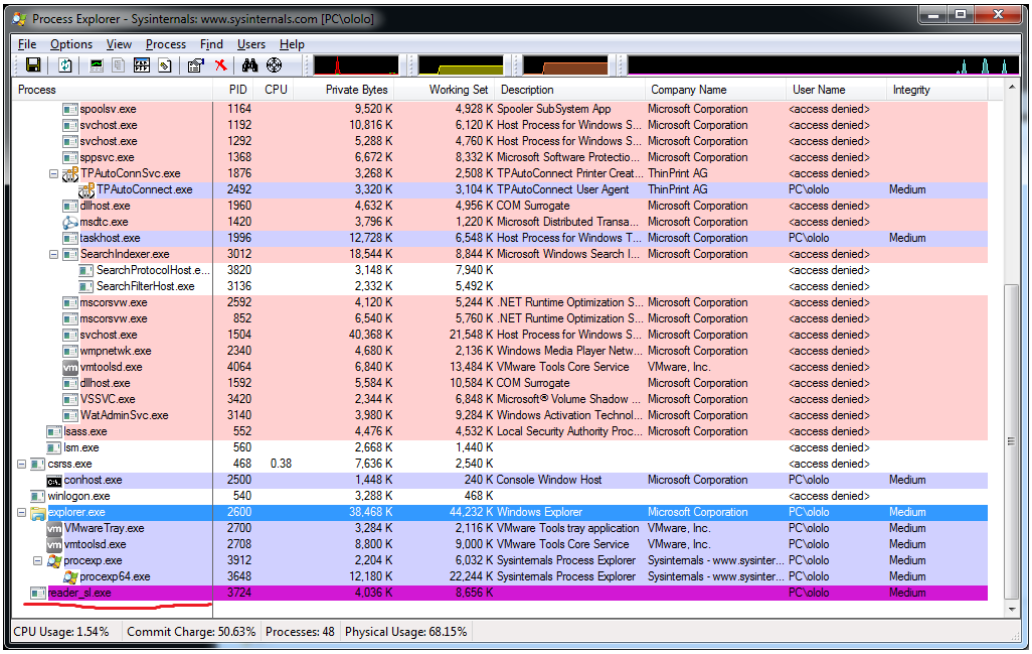
```
int v37; // [sp+98h] [bp-34h]@14
int v38; // [sp+9Ch] [bp-30h]@14
int v39; // [sp+C8h] [bp-4h]@1

v2 = 0;
v33 = 7;
v32 = 0;
v31 = 0;
v39 = 0;
v30 = 7;
v29 = 0;
v28 = 0;
LOBYTE(v39) = 1;
(*(*a2 + 40))(a2, &v34);
if ( (*(*a2 + 36))(a2) < 0 )
  _wassert(L"SUCCEEDED(hr)", L"CNotifyInterface.cpp", 0x2Cu);
if ( (dword_438200 - dword_4381FC) >> 2 )
{
  while ( memcmp((*sub_40106F(v2) + 4), &v34, 0x10u) )
  {
    if ( ++v2 >= (dword_438200 - dword_4381FC) >> 2 )
      goto LABEL_38;
  }
  v3 = *(*sub_40106F(v2) + 104);
  if ( v3 == 1 )
  {
    v14 = DecryptString(L"pnt8");
```

GovRAT supports self-encryption of own body, making the sample analysis fairly complicated for security researchers

Self-Encryption& Anti-Debugging

The sample hides itself in the system under the name of **Adobe Reader Speed Launcher** (reader_sl.exe).





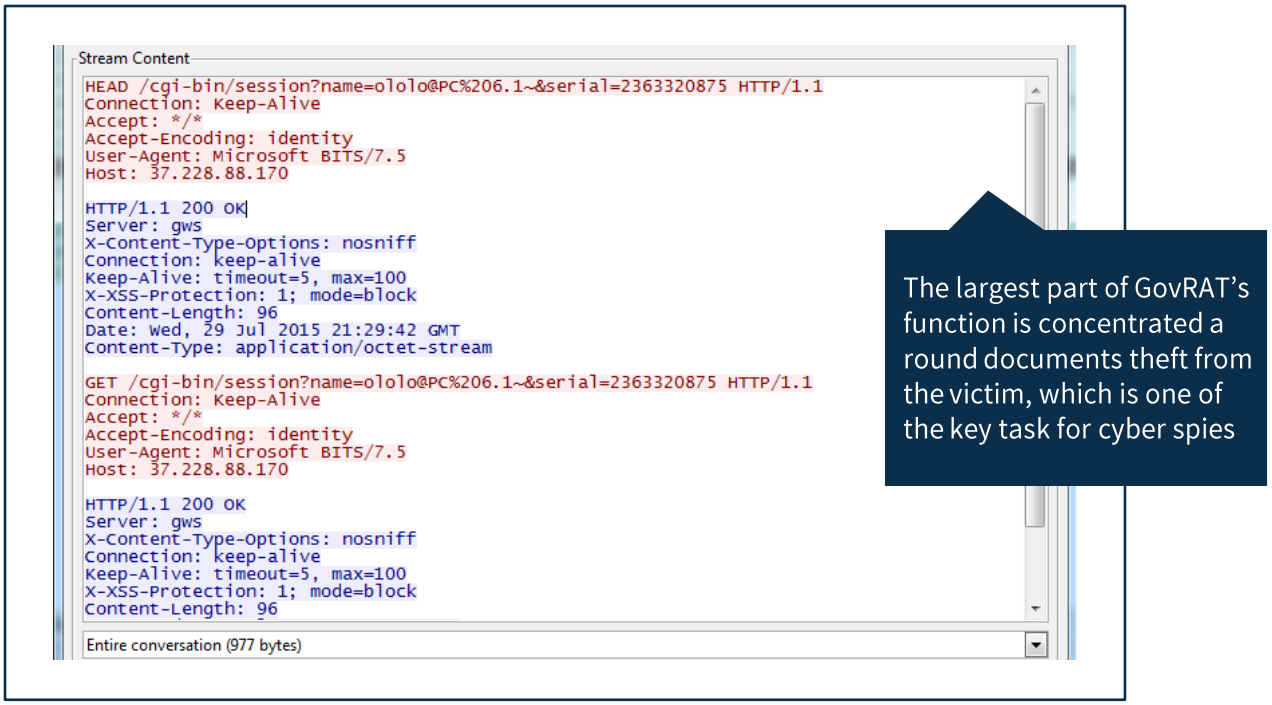
The malware hides in the system as legitimate Adobe process

C&C Network Communications

INFOARMOR
DETECTION IS THE NEW PREVENTION

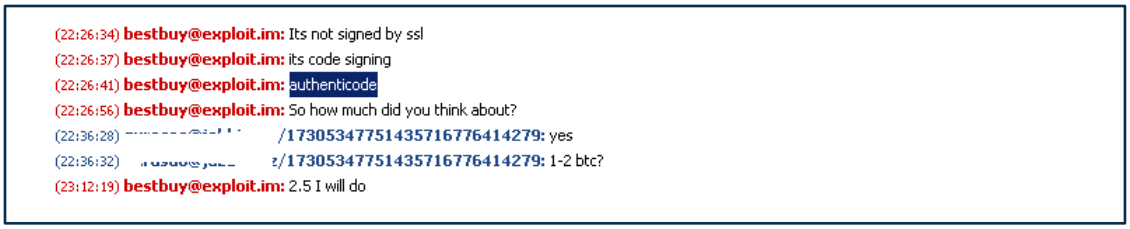
Analyzing network communications of the malware sample, **Microsoft-CryptoAPI/6.1 & Microsoft BITS/7.5** were identified as being used in the User-Agent field."

During the information exchange, **GovRAT** transmits the volume serial number, host name for the infected machine, and active user. The operator may execute commands for files collection by criteria or arbitrary commands execution on the victim.



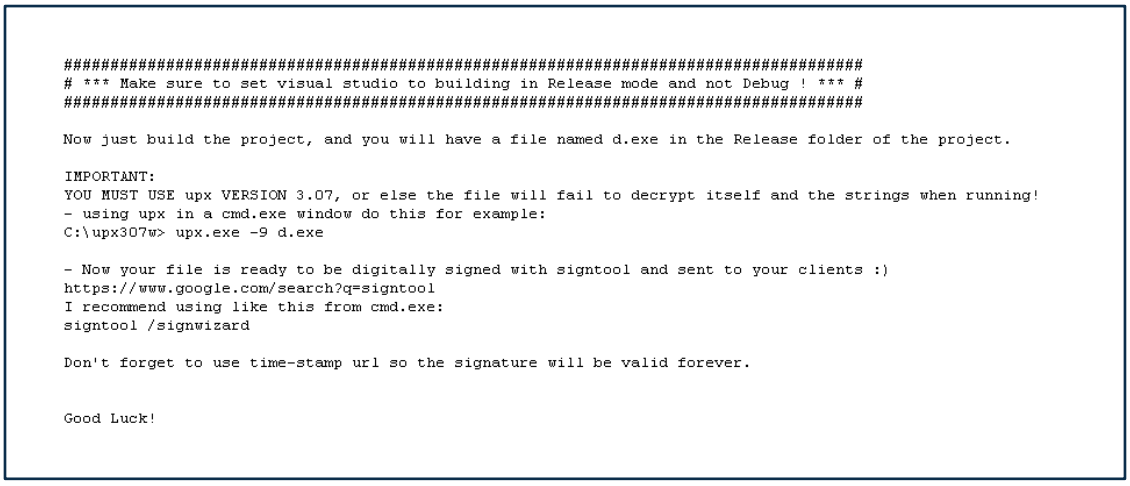
Authenticode Code-Signing Certificates

The author of **GovRAT, "bestbuy,"** removed the post about his malware some time ago and began selling it privately. In addition to **GovRAT**, he also sells code signing certificates using **Authenticode™** technology.



Bestbuy – GovRAT's Author

In order to sign the created binary, **GovRAT** includes special tools for code-signing, such as **Microsoft SignTool**[1] and **WinTrust** in order to ensure that the file is successfully signed.



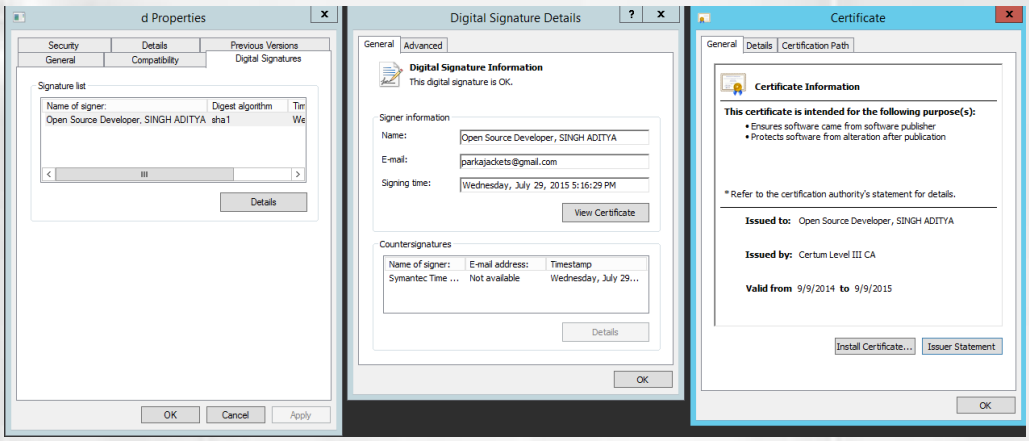
```
################################################################################
# *** Make sure to set visual studio to building in Release mode and not Debug ! *** #
################################################################################

Now just build the project, and you will have a file named d.exe in the Release folder of the project.

IMPORTANT:
YOU MUST USE upx VERSION 3.07, or else the file will fail to decrypt itself and the strings when running!
- using upx in a cmd.exe window do this for example:
C:\upx307w> upx.exe -9 d.exe

- Now your file is ready to be digitally signed with signtool and sent to your clients :)
https://www.google.com/search?q=signtool
I recommend using like this from cmd.exe:
signtool /signwizard

Don't forget to use time-stamp url so the signature will be valid forever.


Good Luck!
```

1 https://msdn.microsoft.com/en-us/library/windows/desktop/aa387764(v=vs.85).aspx

Authenticode Code-Signing Certificates

INFOARMOR
DETECTION IS THE NEW PREVENTION

Analyzed malware sample had a digital signature, issued on Open Source Developer – Singh Aditya (parkajackets@gmail.com) by http://www.certum.pl/certum/main.xml.



All the identified certificates used for malware signing had valid digital signatures

Antivirus Evasion Statistics

INFOARMOR
DETECTION IS THE NEW PREVENTION

The results of code-signing allowed the bad actors to make the malware undetectable from than 30 modern well-known AV[2]:

AntiVir (Avira)	OK
BitDefender	OK
Clam Antivirus	OK
COMODO Internet Security	OK
Dr.Web	OK
eTrust-Vet	OK
F-PROT Antivirus	OK
F-Secure Internet Security	OK
G Data	OK
IKARUS Security	OK
Kaspersky Antivirus	OK
McAfee	OK
MS Security Essentials	OK
ESET NOD32	OK
Norman	OK
Norton Antivirus	OK
Panda Security	OK
A-Squared	OK
Quick Heal Antivirus	OK
Solo Antivirus	OK
Sophos	OK
Trend Micro Internet Security	OK
VBA32 Antivirus	OK
Zoner AntiVirus	OK
Ad-Aware	OK
BullGuard	OK
FortiClient	OK
K7 Ultimate	OK
NANO Antivirus	OK
Panda CommandLine	OK
SUPERAntiSpyware	OK
Twister Antivirus	OK
VIPRE	OK

File Name	d.exe
File Size:	118064
File MD5:	f8d8787c0a984c39a6d58a3e71626bba
File SHA1:	b3dd63f26a812ed8cb89ae9e672916090726ad99

Signed GovRAT has 0 AV detection level

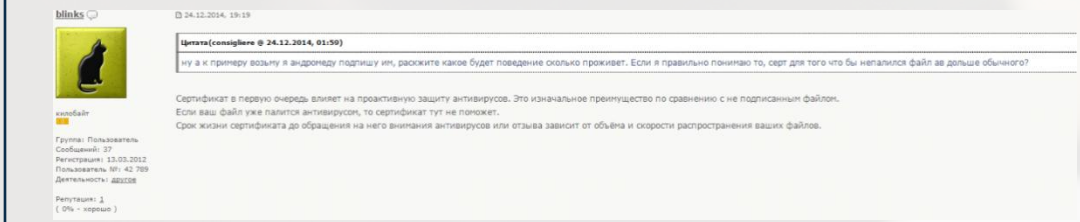
2 http://scan4you.net/result.php?id=a048b_h1kd4j

Code-Signing Certificates Marketplace

INFOARMOR
DETECTION IS THE NEW PREVENTION

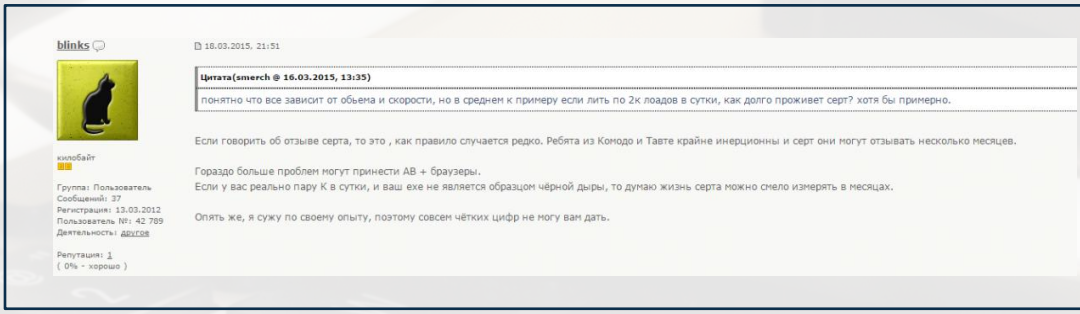
Several other posts were found that promoted code-signing certificates in various underground communities. Bad actors price code signing certificates at $600-900, depending on the issuing company.

The most popular offers are certificates issued by Comodo, Thawte, and GoDaddy, each of which is well respected in the security community and used by many software companies.



Translation (Russian to English):

“ The certificate, firstly, affects proactive defense of antivirus software. It is the key advantage against non-signed file. If your file is already identified by antivirus as malicious, it won’t help you. The timeframe of living of such certificate depends on the attention from antiviruses side, and capacity and speed your distribution of your malware. ”



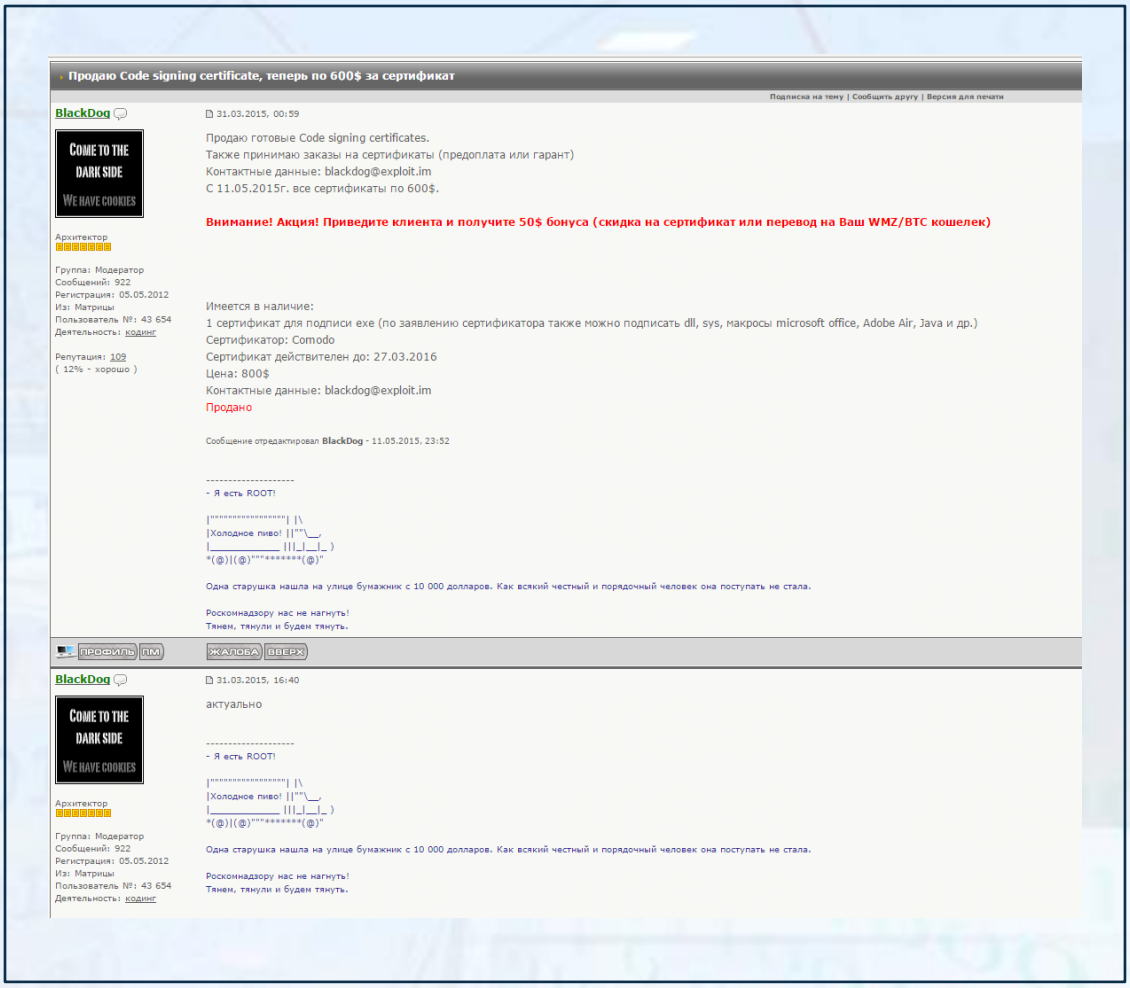
Translation (Russian to English):

“ If we are talking about certificate revoke, it happens very rarely. The guys from Comodo and Thawte are very slow, and they can revoke it several months. The biggest problems can be from AV and Internet browsers side. If you have several thousands victims for infection per day, and your “.exe” is not example of “black hole”, I think, that the life of certificate can be calculated in months. Anyway, I discuss my experience.”

Code Signing Certificates Marketplace

INFOARMOR
DETECTION IS THE NEW PREVENTION

Depending on the bad actors needs, cybercriminals propose to sign not only ".exe" binaries, but dll's, drivers (.sys), Microsoft Office documents, Adobe Air scenarios, and Java files.



Продаю Code signing certificate, теперь по 600$ за сертификат

Подписка на тему | Сообщить другу | Версия для печати

BlackDog

31.03.2015, 00:59

Продаю готовые Code signing certificates.
Также принимаю заказы на сертификаты (предоплата или гарант)
Контактные данные: blackdog@exploit.im
С 11.05.2015г. все сертификаты по 600$.

Внимание! Акция! Приведите клиента и получите 50$ бонуса (скидка на сертификат или перевод на Ваш WMZ/BTC кошелек)

Архитектор

Группа: Модератор
Сообщений: 922
Регистрация: 05.05.2012
Из: Матрицы
Пользователь №: 43 654
Деятельность: кодинг

Репутация: 109
(12% - хорошо)

Имеется в наличие:
1 сертификат для подписи exe (по заявлению сертификатора также можно подписать dll, sys, макросы microsoft office, Adobe Air, Java и др.)
Сертификатор: Comodo
Сертификат действителен до: 27.03.2016
Цена: 800$
Контактные данные: blackdog@exploit.im
Продано

Сообщение отредактировал BlackDog - 11.05.2015, 23:52

- Я есть ROOT!

Одна старушка нашла на улице бумажник с 10 000 долларов. Как всякий честный и порядочный человек она поступать не стала.

Роскомнадзору нас не нагнуть!
Тянем, тянули и будем тянуть.

ПРОФИЛЬ ПМ ЖАЛОБА ВВЕРХ

BlackDog

31.03.2015, 16:40

актуально

- Я есть ROOT!

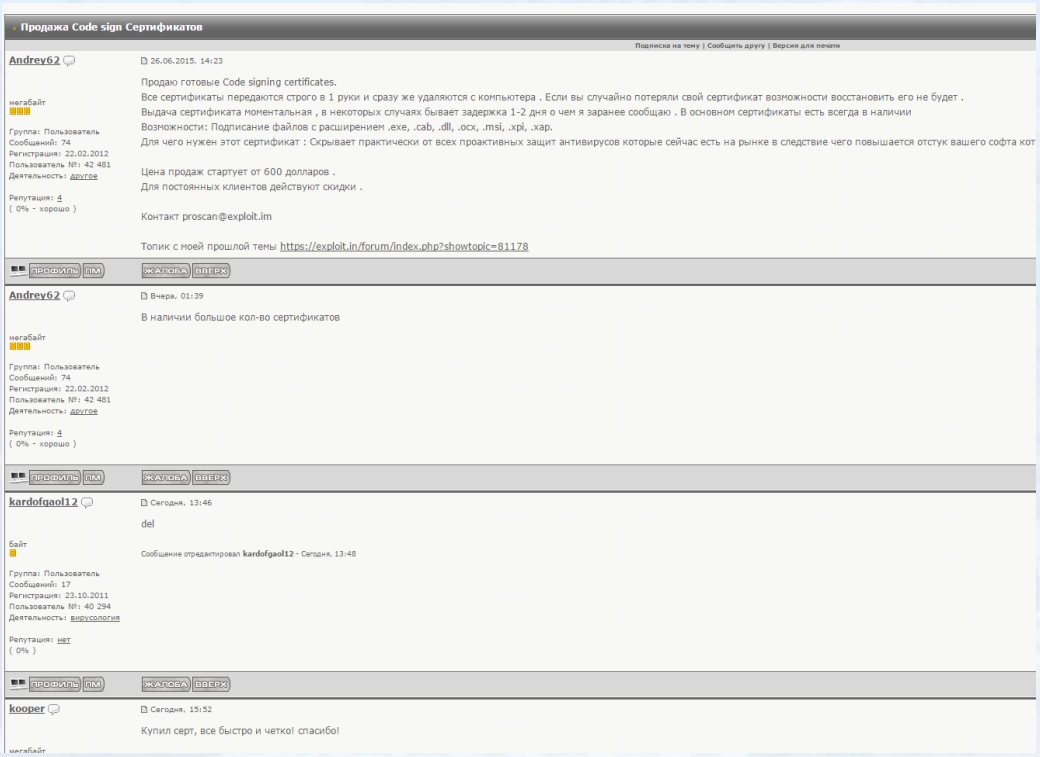
Одна старушка нашла на улице бумажник с 10 000 долларов. Как всякий честный и порядочный человек она поступать не стала.

Роскомнадзору нас не нагнуть!
Тянем, тянули и будем тянуть.

Translation:

" I sell Code signing certificates.
Receive orders on certificates (you need to pay in advance, or through the escrow).
Since 11.05.2015 – all certificates 600$. "

Code Signing Certificates Marketplace


Продажа Code sign Сертификатов

Подписка на тему | Сообщить другу | Версия для печати

Andrey62 — 26.06.2015, 14:23

Продаю готовые Code signing certificates.
Все сертификаты передаются строго в 1 руки и сразу же удаляются с компьютера . Если вы случайно потеряли свой сертификат возможности восстановить его не будет .
Выдача сертификата моментальная , в некоторых случаях бывает задержка 1-2 дня о чем я заранее сообщаю . В основном сертификаты есть всегда в наличии
Возможности: Подписание файлов с расширением .exe, .cab, .dll, .ocx, .msi, .xpi, .xap.
Для чего нужен этот сертификат : Скрывает практически от всех проактивных защит антивирусов которые сейчас есть на рынке в следствие чего повышается отстук вашего софта кот

Цена продаж стартует от 600 долларов .
Для постоянных клиентов действуют скидки .

Контакт proscan@exploit.im

Топик с моей прошлой темы https://exploit.in/forum/index.php?showtopic=81178

Группа: Пользователь
Сообщений: 74
Регистрация: 22.02.2012
Пользователь №: 42 481
Деятельность: другое
Репутация: 4
(0% - хорошо)

ПРОФИЛЬ ЛМ ЖАЛОБА ВВЕРХ

Andrey62 — Вчера, 01:39

В наличии большое кол-во сертификатов

Группа: Пользователь
Сообщений: 74
Регистрация: 22.02.2012
Пользователь №: 42 481
Деятельность: другое
Репутация: 4
(0% - хорошо)

ПРОФИЛЬ ЛМ ЖАЛОБА ВВЕРХ

kardofgaol12 — Сегодня, 13:46

del

Сообщение отредактировал **kardofgaol12** - Сегодня, 13:48

Группа: Пользователь
Сообщений: 17
Регистрация: 23.10.2011
Пользователь №: 40 294
Деятельность: вирусология
Репутация: нет
(0%)

ПРОФИЛЬ ЛМ ЖАЛОБА ВВЕРХ

kooper — Сегодня, 15:52

Купил серт, все быстро и четко! спасибо!

Translation:

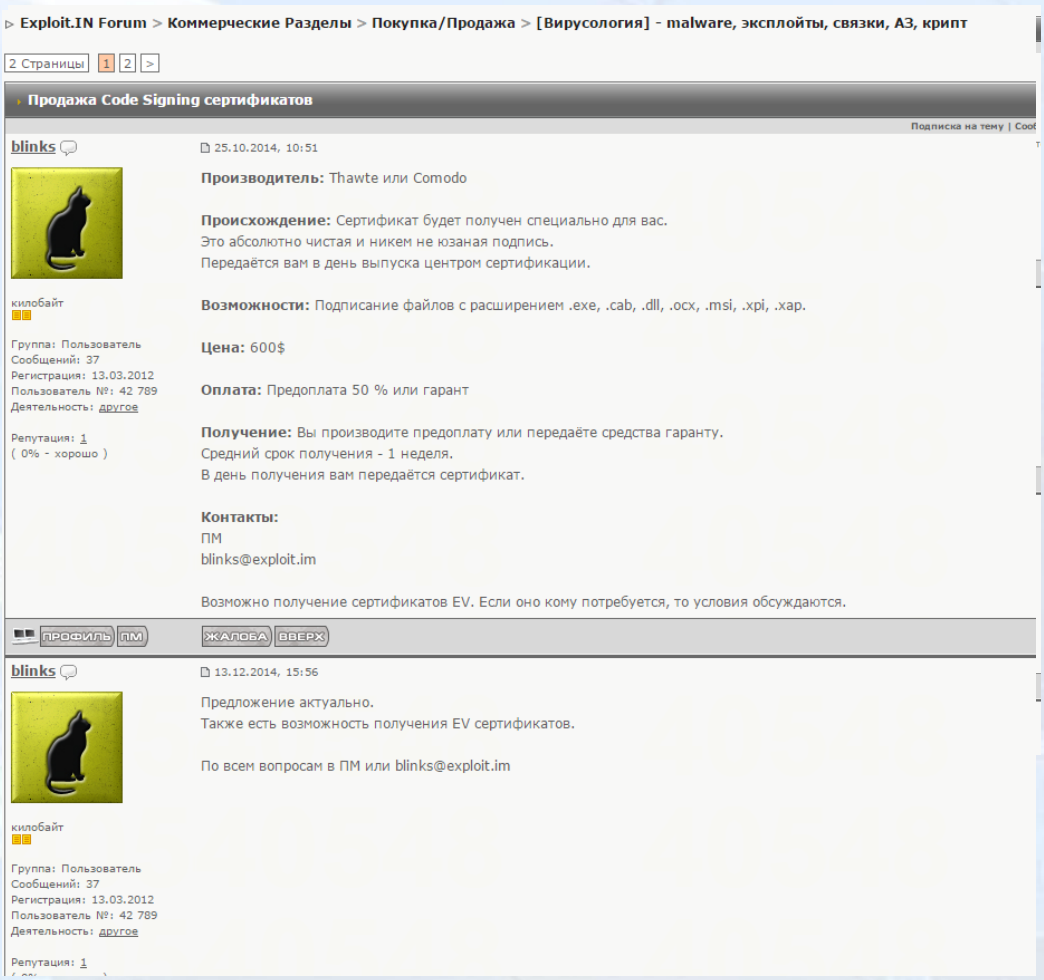
“ I sell ready for use Code signing certificates.

All the certificates are sold only to “one hands”. If your certificate will be lost, there will be no opportunity to recover it. Typically I instantly provide you the certificate after the deal, but in some cases, there can be delay in 1-2 days, I will notify you in advance about it.

I have certificates all the time. Opportunities: Signing of files with the following extensions: .exe, .cab, .dll, .ocx, .msi, .xpi, .xap. For what you need it: It hides your malware from all HIPS of antivirus software, which is currently available on the market.”

Code Signing Certificates Marketplace

INFOARMOR
DETECTION IS THE NEW PREVENTION



▷ Exploit.IN Forum > Коммерческие Разделы > Покупка/Продажа > [Вирусология] - malware, эксплойты, связки, АЗ, крипт

2 Страницы 1 2 >

Продажа Code Signing сертификатов

Подписка на тему | Coob

blinks 25.10.2014, 10:51

Производитель: Thawte или Comodo

Происхождение: Сертификат будет получен специально для вас.
Это абсолютно чистая и никем не юзаная подпись.
Передаётся вам в день выпуска центром сертификации.

Возможности: Подписание файлов с расширением .exe, .cab, .dll, .ocx, .msi, .xpi, .xap.

Цена: 600$

Оплата: Предоплата 50 % или гарант

Получение: Вы производите предоплату или передаёте средства гаранту.
Средний срок получения - 1 неделя.
В день получения вам передаётся сертификат.

Контакты:
ПМ
blinks@exploit.im

Возможно получение сертификатов EV. Если оно кому потребуется, то условия обсуждаются.

ПРОФИЛЬ ПМ ЖАЛОБА ВВЕРХ

blinks 13.12.2014, 15:56

Предложение актуально.
Также есть возможность получения EV сертификатов.

По всем вопросам в ПМ или blinks@exploit.im

килобайт

Группа: Пользователь
Сообщений: 37
Регистрация: 13.03.2012
Пользователь №: 42 789
Деятельность: другое

Репутация: 1

Translation:

“ Vendor: Thawte or Comodo

Source: The certificate will be obtained specially for you. It is absolutely clean and not used signature. It will be provided to you the same day from certification center.

Opportunity: Sign files with .exe, .cab, .dll, .ocx, .msi, .xpi, .xap extensions

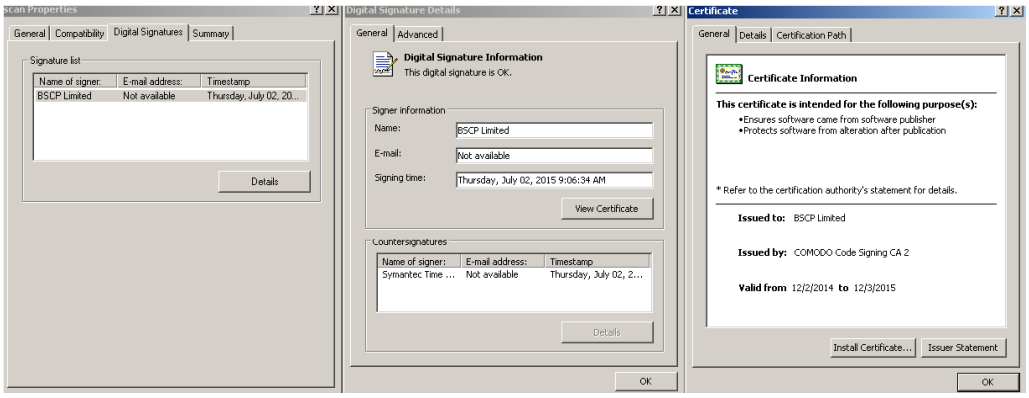
Pricing: 600 USD

Payment: 50% in advance or escrow ”

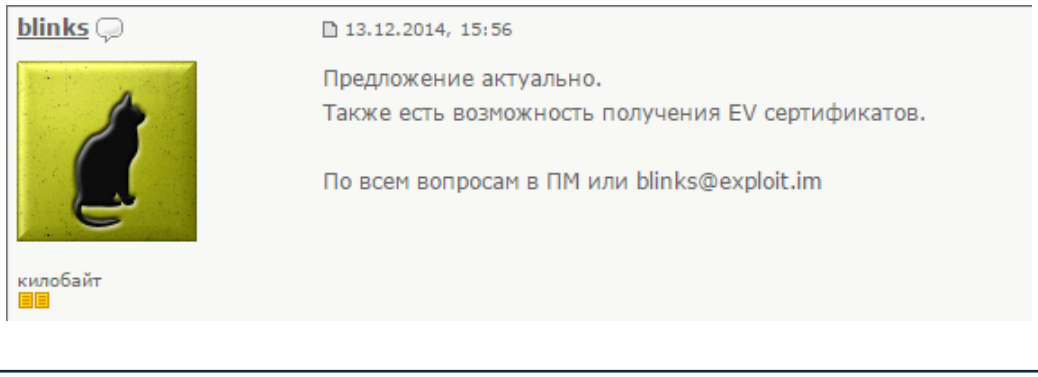
Code Signing Certificates Marketplace

INFOARMOR
DETECTION IS THE NEW PREVENTION

InfoArmor has received an example of a certificate issued on “BSCP Limited” by COMODO.



According to one of the underground vendors named “blinks,” an opportunity to get EV Code Signing. Traditionally, such certificates require full organization validation of the software publisher to guarantee the highest level of security.



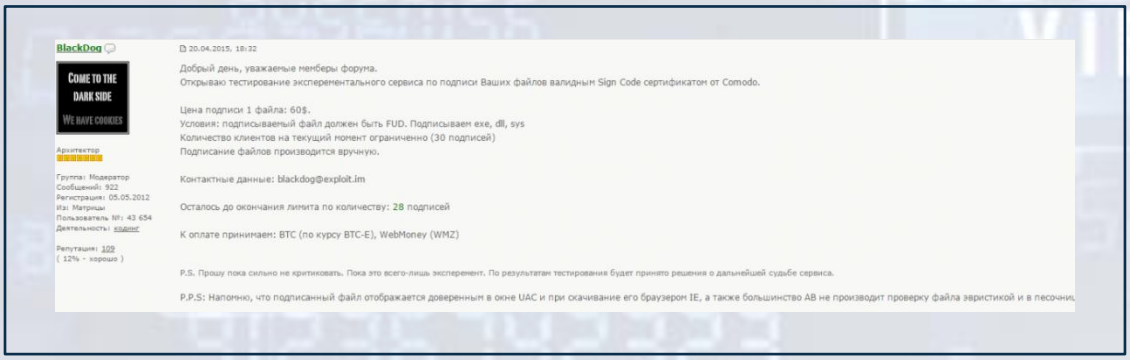
You may also buy EV Code-Signing certificate in the underground

The pricing on this underground service is not inexpensive, but it helps the bad actors perform very efficient, targeted, problem-free APTs.

Alternatively, for budget-conscious malware signers, some bad actors offer a more cost-effective service for just $60. Simply provide a binary for signing, and the bad actor returns a signed malware file.

This lower cost service is not an option for state-sponsored groups or serious bad actors who place a premium on privacy.

Cert4You.org



Translation:

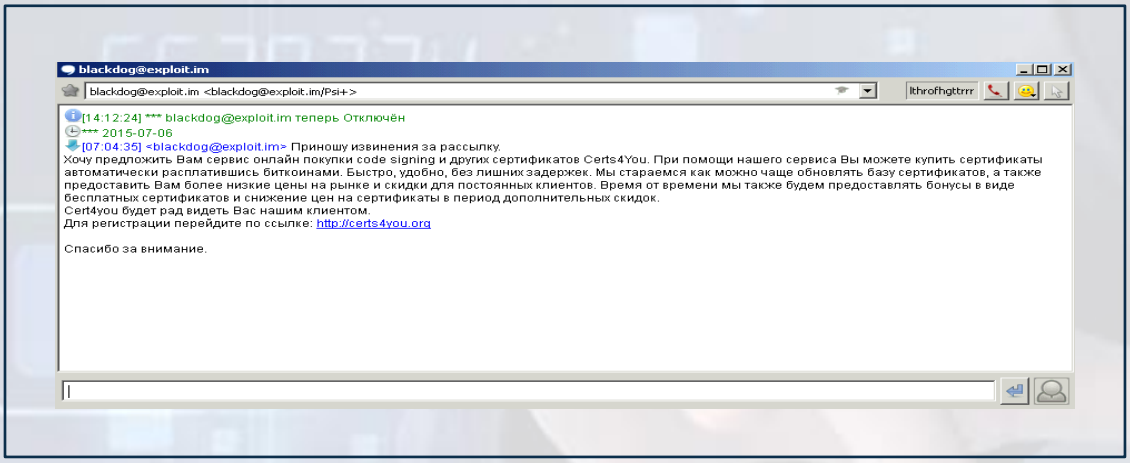
“ The pricing on one file signing is 60 USD.
Conditions: The file should be FUD. We sign only .exe, .dll, and .sys

For today, we have a limit on the number of customers (30 signatures)
The signing is performed manually. We have 28 free signatures for you.

P.S. Just for your information, the signed file shows as trusted in UAC windows, and during downloading, using IE, as well as the most part of AV won’t check it, using their heuristics and sandboxing engines”

Several bad actors have actively discussed the idea of a cybercriminal Software-as-a-Service (SaaS) model providing an opportunity to sign malware in automated fashion using prepared digital certificates.

For example, http://certs4you.org, launched this summer. According to a notification in the underground, the owner of this service is “Blackdog:”



Acting as cybercriminal SaaS, “certs4you” has attracted a lot of interest from the bad actors.

Cert4You.org

INFOARMOR
DETECTION IS THE NEW PREVENTION

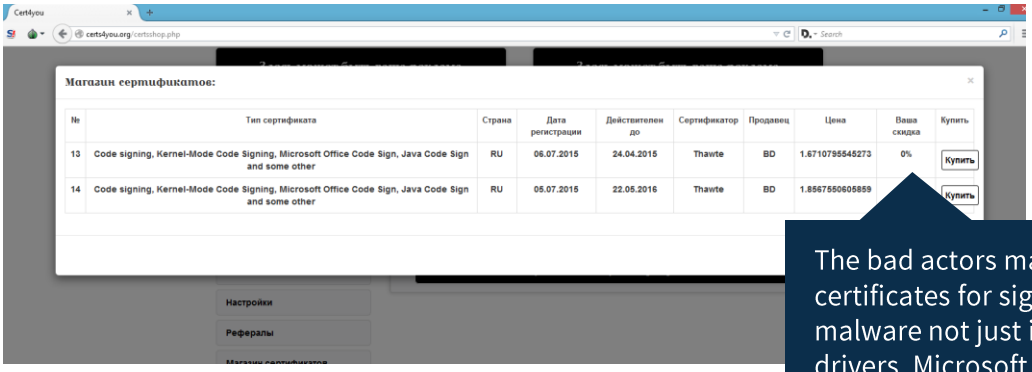
The domain name is registered to a **Belarus citizen – Anatolii Bondar.**

WHOIS:

Domain Name:CERTS4YOU.ORG
Domain ID: D176340506-LROR
Creation Date: 2015-05-24T21:49:51Z
Updated Date: 2015-05-24T21:49:51Z
Registry Expiry Date: 2016-05-24T21:49:51Z
Sponsoring Registrar:PDR Ltd. d/b/a PublicDomainRegistry.com (R27-LROR)
Sponsoring Registrar IANA ID: 303
WHOIS Server:
Referral URL:
Domain Status: clientTransferProhibited – http://www.icann.org/epp#clientTransferProhibited
Domain Status: serverTransferProhibited -- http://www.icann.org/epp#serverTransferProhibited
Registrant ID:DI_44324447
Registrant Name:Anatolii Bondar
Registrant Organization:Certs4you
Registrant Street: ul.Nikitina 13
Registrant City:Minsk
Registrant State/Province:
Registrant Postal Code:93100
Registrant Country:BY
Registrant Phone:+375.9451263548
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email:certs4you@mail.ru
Admin ID:DI_44324447
Admin Name:Anatolii Bondar
Admin Organization:Certs4you
Admin Street: ul.Nikitina 13
Admin City:Minsk
Admin State/Province:
Admin Postal Code:93100
Admin Country:BY
Admin Phone:+375.9451263548
Admin Phone Ext:
Admin Fax:
Admin Fax Ext:
Admin Email:certs4you@mail.ru
Tech ID:DI_44324447
Tech Name:Anatolii Bondar
Tech Organization:Certs4you
Tech Street: ul.Nikitina 13
Tech City:Minsk
Tech State/Province:
Tech Postal Code:93100
Tech Country:BY
Tech Phone:+375.9451263548
Tech Phone Ext:
Tech Fax:
Tech Fax Ext:
Tech Email:certs4you@mail.ru
Name Server:NS35.HOSTIA.NAME
Name Server:NS36.HOSTIA.NAME

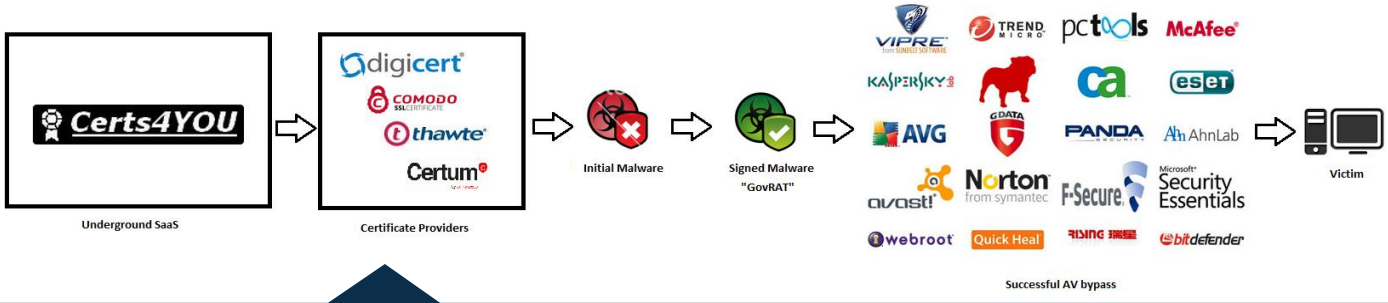
Process Scheme

The service provides a list from which a bad actor can choose the certificate for malware signing, issued by **Comodo, Thawte, DigiCert and many other certificate providers:**



The bad actors may use digital certificates for signing their own malware not just in .exe files, but drivers, Microsoft Office documents, Java content and many other file types

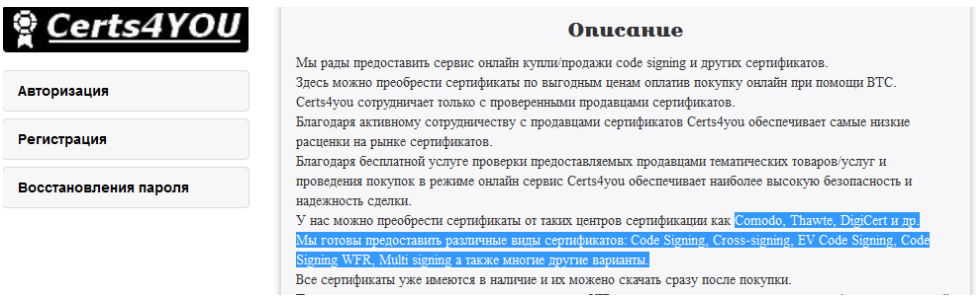
According to the intelligence surrounding **GovRAT**, successful APT variants have been launched against government and large enterprise targets.



Typical process scheme, allowing to prepare malware for APT in few minutes.

Using various operatives, **InfoArmor** has analyzed several samples of digital signatures used by bad actors for code signing.

Subsequent intelligence gathered verified that many of the certificates secured by bad actors and **underground SaaS services** as “Certs4You” were received through resellers. Weak identification and due diligence procedures facilitated the submission of fake documents for exploitation.



The bad actors provide digital certificates from world known certificates providers, such as Comodo, Thawte and Digicert

Indicators of Compromise

INFOARMOR
DETECTION IS THE NEW PREVENTION

Indicators of Compromise (IOC)

InfoArmor has obtained several samples of the identified malware in order to document the indicators of compromise (IOC) for mitigation of further attacks. In most cases, the bad actors have used one certificate per malware sample. Such an approach helps to organize long-term APT campaigns targeting a variety of organizations, and prevent any identification of the source of the attack by AVs.

File Size: 118064
File MD5: f8d8787c0a984c39a6d58a3e71626bba
File SHA1: b3dd63f26a812ed8cb89ae9e672916090726ad99

File Size: 135056
File MD5: b7a5402985d5987115abe9099a363688
File SHA1: c82fefd7d399e9da6b934818dd18e2444222a741

File Size: 118151
MD5: 5e943aab3dd6cb5bb52f4857dc5deb53
File SHA1: 8261bf6ce32d2d29460f24c2946dd8994ab27049

File Size: 115083
File MD5: 0b8b828be2dfb247ae6d4f778d291d8f
File SHA1: 7d3f058c2e3bb585ad8b4bd7f3256c479dd049c0

File Size: 124656
MD5: 779ea144b7e8f60f4ccd277cb29f74f0
File SHA1: 8c03997f140d43170ccc50f15e83d214be57f84b

File Size: 124656
File MD5: 75bc93abfeb36d506fa9a92490630051
File SHA1: 7eb62f39da877364445bb1a9898a391ee5d3b619

INFOARMOR
DETECTION IS THE NEW PREVENTION

About InfoArmor

InfoArmor offers industry-leading identity and cyber intelligence services that help our clients fight emerging fraud and advanced cyber threats. We combine an unparalleled global research network with big data analysis, actionable intelligence and customized service to meet clients' dynamic security needs. From employee to enterprise, InfoArmor is redefining how organizations fight fraud and combat an evolving threat landscape to mitigate risk on multiple levels. Today, more than 600 businesses and government agencies, including 50 of the Fortune 500, use PrivacyArmor, our employer identity protection solution, or our advanced threat intelligence platform to improve their data security posture. For more information visit *ati.infoarmor.com*.

Contact Us

InfoArmor, Inc.
7001 N Scottsdale Road, Suite 2020
Scottsdale, AZ 85253

(800) 789-2720 | (480) 302-6701
Monday - Friday, 6 a.m. - 6 p.m. (Pacific)